Information Commissioner's Office
Promoting public access to official information
and protecting your personal information

Data Protection Technical Guidance
Radio Frequency Identification

This technical guidance note is aimed at those using or contemplating using RFID technology. It gives a brief summary of the technology and its usage before looking at how the Data Protection Act 1998 ("the Act") applies to its use.

1. Technical summary

Radio frequency identification (RFID) tags provide a means of identifying and locating items using radio signals. An RFID system consists of:

- a radio-transmitter "tag" (or "transponder"), including a microchip and antenna, and
- a reader, or "interrogator", with an antenna.

The reader emits radio frequency waves, which are received by the tag's antenna. When scanned by a reader, the tag communicates information from its memory in analogue form, and this is then converted to digital data by the reader. Information can be stored both on the tag itself and in a "back-end" computer system to which the tag refers.

Tags may be *active* or *passive*. An active tag has its own battery supply to power its communication with the reader; a passive tag uses the power created by the reader. For this reason passive tags can be very small, but their read range is reduced. Larger, more expensive active tags are likely to be used for tracking high value goods that require long-range scanning, for example during transit by rail. The operating range of RFID tags depends on the frequency used, varying from a few centimetres for low frequency tags to over a hundred metres for microwave tags. Currently the cost of RFID tags is prohibitively high for many potential users, but industry experts anticipate that prices will fall as take-up of the technology becomes more widespread.

RFID tags overcome some of the limitations of barcodes. Barcodes are read using a close range optical barcode scanner, and typically provide information only at the generic product level, but RFID tags ascribe a unique identifier to each individual item, and these can be read out of the line of sight. RFID tags can also supply more data than a barcode, either using a pre-loaded read-only memory or a static random access memory. In typical supply chain and consumer packaging applications a tag's memory will contain only an electronic product code (EPC), but this code can be associated with data in an online database.

The EPC is a globally unique reference number found on an RFID tag. It is divided into numbers which identify the manufacturer, product type and unique item. Industry standards for the EPC are being developed by EPCglobal, a not-for-profit organization that works with companies to encourage the adoption of EPC technologies.

2. Current usage

The principal use of RFID at present is in supply chain management. RFID tags are used to track vehicles between depots and pallets of goods from warehouses to stores. Tagging at item level has been deployed by major retailers and manufacturers to monitor stocks that are running low. RFID is becoming more frequent in prepaid travel cards, such as the Oystercard used for London's transport system. Each Oystercard has a unique identity number linked to the registered owner, and records the routes and times of each journey for which the card is used. This application has developed into a widespread contactless payment system. Customers need only move their card or phone over a reader for it to register payment and automatically deduct the price or fare from the customer's account, or check that it is within a prepaid limit. Payment by RFID-enabled "smart" card, credit card and even mobile phone has been introduced in points of sale in several countries.

The US State Department has announced that passports issued after October 2006 will be embedded with RFID chips storing personal data including biometric information. Other current and developing uses of RFID tags include the tracking of livestock, monitoring of passenger baggage at airports, and unique identification of drugs and event tickets to prevent counterfeiting.

Pilots of RFID include a scheme in Seattle where tags triggered readers to broadcast marketing messages tailored to the tag holder's preconfigured profile, and a Japanese trial of tagged bracelets designed to make children's school journeys safer. In a few cases, individuals have chosen to have RFID tags implanted in their skin, for example, to access VIP services at a nightclub. It has been suggested that such subcutaneous tags might help to track hospital patients with mental health conditions.

There is some debate as to how prevalent RFID will become. There seems little doubt that its use in supply chain applications will continue to increase in the next few years. But opinion is divided on whether RFID technology in retail will ever extend to a tag on every consumer item purchased. For this to happen, prices must continue to fall, and many believe that until the cost of a single tag is very low, few retailers will be able to achieve a return on investment with RFID on any but the most valuable products.

Nevertheless, some in the industry anticipate a future where everyday objects and appliances are connected to the internet, and each other, via RFID tags. This so-called "internet of things" will enable people to interact more with their environment, and their belongings with each other. For example, "smart" fridges could automatically reorder products that they registered as running low, intelligent watches could prompt users who leave the house without their keys and hotels could have "smart" mini-bars which automatically bill customers when drinks are removed.

3. How does the Data Protection Act apply?

The Data Protection Act 1998 concerns the processing of personal data. Any electronically held information relating to an identified or identifiable individual is personal data. It is not easy to define exactly when an individual is identified, but identifying someone does not necessarily mean being able to ascribe a name and address to them. If a person is uniquely distinguished from all others within a relevant group, he will be identified.

There are two ways in which personal data might be processed using RFID. First, personal data may be stored on the tags themselves, or linked to a database containing personal data. Second, if tags on individual items can be used to identify the individual associated with the item, they will be personal data.

Scenario 1: Tag stores or is linked to personal data

In applications where personal data is stored using RFID, the Act will apply. For example, contactless payment cards carry a link to the holder's personal account information. Similarly, smartcards used for travel might be linked to information about the holder's recent journeys, and passports or identity cards to biometric information.

Scenario 2: Tag does not store personal data but individuals are identified by it

In some applications people will be identified by RFID tags. For example, in the Japanese program to make children's school journeys safer, pupils wore bracelets containing an active tag. Software was used to locate each child within a given area based on the tag's signal strength. The purpose of the system was to uniquely identify each child by the number of his tag.

But people might also be identified by RFID even where this was not the original intention. If someone always wore a watch that carried an RFID tag, the serial number for the watch's tag could also serve as a serial number for the wearer. While RFID tags on individual products will not constitute personal data in a customer's shopping basket, they could become personal data in circumstances where they enable the identification of individuals.

A tag could also be associated with an identified individual if product data was subsequently combined with personal data from, for example, supermarket loyalty cards. This could be done at points of sale or if customers use cards to access special services, such as listening to CDs or viewing product information.

In other situations, there will be no data protection implications. In most of the current applications of RFID, there are few data protection concerns because the tags do not store or communicate personal data, and are not linked to an identifiable individual. For example, the tags used currently in the retail sector

contain only an EPC and are not commonly found at item level so consumers will rarely come into contact with them.

It is recommended that RFID users do not collect or store personal data if it is not necessary to do so. Keeping track of the popularity of products, for example, will not necessarily require the recording of data about specific shoppers' buying habits. Users will need to be aware that where it may be possible to identify someone using data from RFID systems coupled with information available elsewhere, personal data will be processed. For example, RFID tags have been used in supermarkets to generate data about how often certain products are removed from shelves. Usually this data will be general and not relate to individuals. If such information were linked to identified individuals, however, it would constitute personal data. This might be done, for example, by combining data from RFID tags with individuals' images captured on CCTV.

Where personal data is collected, generated or disclosed using RFID either directly or indirectly, the Act will apply. RFID users will have to give special consideration to the data protection principles:

- Fair processing

In order to comply with the fair processing requirements of the Act, those collecting personal data with RFID will have to give notice of the presence of RFID tags on products and of readers, and explain the implications. They will have to tell consumers what personal information is being collected, by whom, and for what purpose. The Act also requires them to consider what other information would need to be provided. It is likely that disclosures of information outside normal expectations would need to be explained. In some circumstances it might also be necessary to tell customers how to disable or remove tags, for example if a tag has been left on a product after purchase.

RFID users must also tell individuals if tag serial numbers were to be linked with personal information and thus become personal data.

- Use limitation

Personal information should only be collected for specified legitimate purposes, so companies using RFID should be wary of any "function creep" in their deployment.

- Data quality

Users of RFID need to ensure that any personal data is accurate and kept up to date. Personal information beyond that necessary for the purpose of the system should not be collected.

- Data retention

Personal information should not be kept for longer than is necessary for its specified purpose.

- Security

  Users of RFID will need to ensure the security of any personal data stored on them or linked to them.

Data controllers will have to consider the logistics of compliance with the Act before adopting the technology. In a world of “ubiquitous computing”, security and privacy safeguards should be built into the architecture of RFID systems, rather than added on later.

4. Specific data protection concerns

Security

It will be the responsibility of RFID users to prevent any unauthorised access to personal information.

One concern is a practice that has become known as “skimming”. Since a transponder’s signal can be picked up by any compatible reader, it is possible for RFID tags to be read by unauthorised readers, which could access personal information stored on them. Users can guard against skimming by using passwords. The EPCglobal Class 1 Generation 2 RFID specification enables the use of a password for accessing a tag’s memory. However, these are not immune to “hacking”. Most RFID systems require a short distance between tag and reader, making it difficult for “rogue” readers to scan tags but this could nevertheless be done in a situation where people are naturally at close range, for example, on a crowded train. The nominal read range of some tags can also be extended by the use of more powerful readers.

It is also possible to read part of a tag’s number by eavesdropping merely on a reader’s communication with a tag. Readers, with a much higher power output than tags, can be read at much greater distances. While some RFID applications might not need communication between tag and reader to be encrypted, others that process personal and especially sensitive personal data will need an adequate level of encryption to safeguard the data being processed.

In most cases “skimmers” would also need a way of accessing the external database containing the personal data, but in some cases inferences might be made about someone from information which in itself does not relate directly to him. If a person leaves a store having purchased items carrying RFID tags that have not been disabled, he carries with him a potential inventory of his possessions. This would enable someone with a suitable reader and knowledge of EPC references to discover what items he was carrying at a given time. Sensitive personal data about a person’s illness, for example, might be unknowingly revealed by him via the EPC referring to the medication in his pocket.

An insufficiently secure RFID chip could also be “cloned”. By copying personal data stored on the RFID chip of an identification card, a person could for

practical purposes steal the identity of the cardholder. If the information on the database (e.g., a fingerprint) is checked only against the information on the card, rather than directly against the person himself, a criminal would not need to access the information stored on the database.

Cryptography has been suggested as a way to combat skimming. A tag could communicate not just one number, but several “pseudonyms” in rotation. An authorised reader would store the full set of pseudonyms in advance, recognising each as a communication from a single tag. An unauthorised reader could not correlate different appearances of the same tag.

Monitoring

People’s movements

Travel smartcards such as the Oystercard collect information about people’s journeys which is then stored on a linked database. This information is used to tie together the journeys made on an individual travel card and improve journey planning. People’s movements should not be tracked in this manner without a legitimate reason: for example, the personal data collected from a travel card should be relevant and proportionate to the needs of journey planning and customer service. Anyone who is subject to such tracking with RFID should be informed of this, and consent will be needed for any tracking that goes beyond what people would expect for a given legitimate purpose.

Employees’ work

The technology has been used by employers in Japan to monitor the efficiency of their employees. Workers carry mandatory RFID tags whose data is analysed to show how much each individual contributes to production. While such a system might raise concerns about trust between employer and employees, the data protection issue is whether employers have a legitimate reason for such monitoring and whether their use of personal data is proportionate to the interests it serves. Employers should refer to the Employment Practices Code for more detailed guidance on monitoring at work.

Profiling

RFID can enable stores to build up individual profiles of their customers’ shopping habits. For example, tagged tokens for operating shopping trolleys have been given to customers that allow the monitoring of their purchases. This may or may not involve personal data, because valuable consumer information could be created without associating details with identified individuals.

If individual profiles were constructed by stores in this way they could be used to target marketing directly to people whose preferences had been ascertained. For stores to adhere to the fair processing requirements of the Act in these cases they would have to inform customers not only that

consumer profiling is taking place, but also that profiles might be used for direct marketing. They would also have to provide customers with a means of opting out of such direct marketing.

It is important that any similar use of RFID in retail that involves the personal data of customers is done openly, and that customers understand how their information is being used. Any use that lies outside the normal expectations of customers will not be fair. If tags remained on a person's purchases after leaving a shop, for example, other stores might also be able to scan these for the direct marketing of similar products. While customers might expect stores to scan their own RFID tags for anti-theft purposes, they are unlikely to expect purchases from other shops to be scanned, or for this information to be used for marketing.

5. Technical solutions

The simplest way of addressing privacy concerns about RFID is to ensure that any tags on individual items are removed or disabled at the point of purchase. While the removal of a tag is a more visible process from the buyer's point of view, it also removes the possibility of using the tag if the product is returned.

The predominant privacy mechanism for RFID is the "kill" command. When a reader transmits the command with an associated password, the tag switches to a state in which it is permanently unable to respond to interrogation. Like the option of removing the tag, this mechanism rules out future use of the tag even for the consumer's benefit, for example for the purposes of a guarantee or refund. Kill commands generally use a 32-bit password, the simplicity of which some have argued makes tags too susceptible to sabotage. For these reasons other methods of disabling tags have been proposed. These include:

- "blocker" tags, which send a confusing response to a reader's signal, making meaningful reading of genuine tags impossible;
- "clipped" tags, involving the temporary removal of the tag's antenna, which preserve the tag's functionality while drastically reducing its read range, and
- radio frequency shielding, such as will be used to prevent the new US passport being read unless it is opened.

The technical solution adopted should take into account the nature of the data and the harm that is likely to result from any misuse.